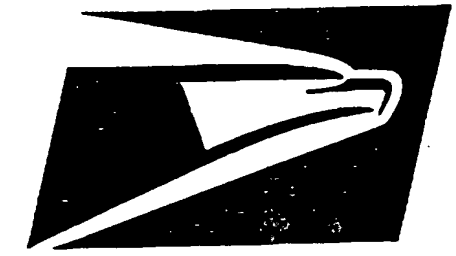
XP-002137734

P.D. 13-06-1996
p. complete = (41)

INFORMATION BASED INDICIA PROGRAM
POSTAL SECURITY DEVICE SPECIFICATION



June 13, 1996

Prepared for:
The United States Postal Service (USPS)
Engineering Center

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION AND BACKGROUND

1.1 Introduction

This specification defines the proposed requirements for a Postal Security Device (PSD) that will provide security services to support the creation of the new "information based" postage postmark or indicium that will be applied to mail being processed using the Information Based Indicium Program (IBIP). The United States Postal Service (USPS) is issuing this specification to obtain comments from its customers and industry.

The IBIP is expected to support new methods of applying postage in addition to, and eventually in lieu of, the current approach, which typically relies on a postage meter to mechanically print indicia on mailpieces. The term "host" is used in this specification to refer to the host computer system or the meter, as appropriate. PSDs are not expected to differ between computer-based and meter-based applications.

1.2 Structure of This Specification

This specification is organized into five sections and two appendices. The following is an overview and general description of each section and appendix.

- **Section 1 - Introduction and Background:** This section gives readers a brief introduction to the PSD specification.
- **Section 2 - PSD Overview:** This section presents an overview of PSD functions.
- **Section 3 - PSD and IBIP Functions:** This section specifies the PSD core functions, including digital signature, register management, and initialization. This section also describes the role that the PSD plays in IBIP device authorization, finance, indicium creation, and device audit functions.
- **Section 4 - PSD Physical Requirements:** This section documents the physical requirements for the PSD. It covers PSD contents, software, watchdog timer, tamper resistance, access control, key handling, and input/output requirements.
- **Section 5 - PSD Test Requirements:** This section specifies the test requirements for the PSD.
- **Appendix A - Host System Security Requirements:** This appendix addresses host system security requirements that must be understood by developers of the PSD.
- **Appendix B - List of Acronyms.**

1.3 Interpretation of Requirements

The requirements presented in this document are composed of statements containing the word "shall." Requirements using the word "shall" are to be interpreted as a mandatory specification. Other statements use the words "should" or "may." Statements using the word "should" are to be interpreted as recommendations; statements using the word "may" are to be interpreted as design-related or functional options to consider for implementation purposes.

This specification documents both DSA (Digital Signature Algorithm) and RSA encryption requirements for the PSD, but does not exclude other methods. Any statements herein that specify requirements for DSA or RSA encryption only apply if the PSD is designed to use such signature methods.

1.4 Reference Documents and Resources

The proposed requirements and specifications included in this document are supported by the primary resources:

- USPS Domestic Mail Manual (DMM) September 1, 1995.
- Federal Register, Part V, 39 CFR Parts 111 and 501, Manufacture, Distribution, and Use of Postage Meters; Final Rule June 9, 1995.
- Uniform Symbology Specification PDF417 July 1994.
- Digital Signature Standard - FIPS PUB 186 May 19, 1994.
- Secure Hash Standard - FIPS PUB 180-1 April 17,1995.
- Security Requirements for Cryptographic Modules - FIPS PUB 140-1 11 January 1994.
- Cryptographic Module Validation Program Announcement July 17, 1995.
- Information Based Indicium Program Indicium Specification June 13, 1996.
- Information Based Indicium Program System Specification, (to be issued).
- PKCS #1: RSA Encryption Standard version 1.5 November 1, 1993.
- RFC 1321, The MD5 Message Digest Algorithm April 1992.

1.5 Patent and License Considerations

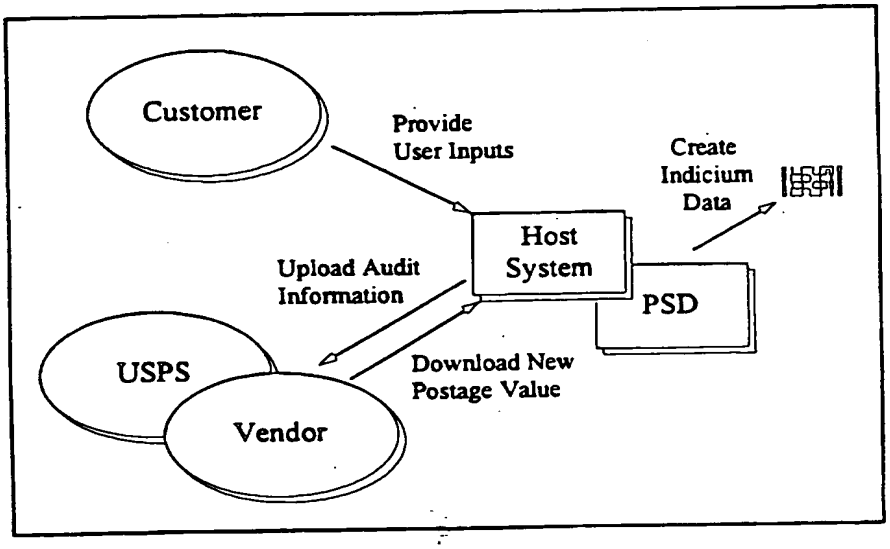
The requirements contained in this specification may be subject to patent claims by various organizations. It shall be the responsibility of the vendor to obtain any required rights, such as licenses, to use the approach chosen.

2. POSTAL SECURITY DEVICE (PSD) OVERVIEW

The Postal Security Device (PSD) provides security-critical functions for IBIP customers. The PSD will be a hardware component for use with either a computer-based or postage meter-based host system. Each PSD will be a unique security device. The PSD core security functions are cryptographic digital signature generation and verification, and the secure management of the registers that track the remaining amount of money available for indicium creation (descending register) and the total postage value used by this PSD (ascending register). To ensure the security of IBIP processes, certain core security functions, which are further described in Section 2.1, must be performed by the PSD. In order to securely perform these functions, the PSD will be a tamper-resistant device that will contain an internal random number generator, various storage registers, a date/time clock, and other circuits necessary to perform these functions. The PSD will be compliant with FIPS 140-1 and will be validated through the National Institute of Standards and Technology (NIST) Computer Systems Laboratory's Cryptographic Module Validation Program.

The PSD core security functions will support the implementation of the IBIP device authorization, finance, indicium creation, and device audit functions, which are further described in Section 2.2. The PSD ensures that only authorized IBIP customers are able to apply a valid indicium to a mailpiece. Figure 2-1 illustrates the role that the PSD plays in the creation of indicia.

Figure 2-1. PSD Role in IBIP Indicia Creation



2.1 Core PSD Security Functions

2.1.1 PSD Initialization

PSD initialization is the process of loading the unique device identifier and the vendor's X.509 certificate into the PSD. (The initialization information also must be entered in the IBIP customer database.) The PSD must be initialized before it can be authorized for customer use.

2.1.2 PSD Digital Signature Function

A digital signature is a process that enables the recipient of a signed message to verify that the contents of the message have not been modified. The PSD will generate a digital signature for each indicium. It also will generate a digital signature to ensure that the device audit information has not been modified. The PSD will be required to verify the digital signature of the USPS for IBIP finance functions.

2.1.3 PSD Register Management Function

Register management refers to the ability of the PSD to securely manipulate the ascending and descending registers. The PSD will use register management to support the IBIP finance, indicium creation, and device audit functions as discussed in Section 3.2.

2.1.4 PSD Functional Allocation

The PSD core security functions will support the implementation of the IBIP requirements. The matrix of PSD security functions and IBIP functions is provided in Table 2.1-1.

Table 2.1-1. PSD Security Functions and IBIP Functions Matrix

PSD Security Functions	IBIP Device Authorization	IBIP Financial Functions	IBIP Indicium Creation	IBIP Device Audit
Initialization	✓			✓
Digital Signature	✓	✓	✓	
Register Management		✓	✓	

2.2 IBIP Functions

2.2.1 IBIP Device Authorization

The IBIP authorization process ensures that only an authorized device can support the creation of a valid indicium. The vendor will authorize a PSD for use by a specific licensed customer. Once a PSD is authorized, the finance functions must be performed before the first indicium is created.

2.2.2 *IBIP Finance*

The IBIP finance function will download postage value into the PSD. Prior to downloading postage into the PSD, the customer must deposit sufficient funds with the USPS. To initiate the secure downloading of postage, the PSD will generate a request message for postage value download. Once a download message is received, the PSD will be required to verify the digital signature for the message. After the signature has been verified, the PSD will increase the value contained in the descending register by the added postage value amount contained in the message. The PSD will upload a status message and device audit information to the USPS that reflects the new value of the descending register and the current value of the ascending register.

2.2.3 *IBIP Indicium Creation*

The PSD and the host system will jointly perform functions necessary to create a valid indicium in accordance with the IBIP Indicium Specification. The PSD will accept input from the host system and use data from its internal storage to create signed data elements for selected fields in the indicium.

2.2.4 *IBIP Device Audit*

The device audit function allows the USPS to ensure proper use of the PSD. To ensure such use, the PSD will create an appropriate device audit message and output it to the host system for transfer to the USPS. The PSD will provide a watchdog timer function. This function will preclude indicia creation if the PSD has not been adequately audited by the USPS.

3. PSD FUNCTIONAL REQUIREMENTS

Functional requirements for the PSD are specified in two subsections below. Section 3.1 identifies core PSD functional requirements. Section 3.2 identifies how the core PSD functions are to be applied to satisfy overall IBIP requirements.

3.1 Core PSD Functional Requirements

This section presents requirements for the core PSD functions that will be applied in various combinations to implement security services for the IBIP functions presented in Section 3.2. In the event that vendors wish to extend the PSD to applications beyond IBIP, the core functions also could be used to support these applications.

3.1.1 PSD Digital Signature Functions

The PSD may implement either DSA, RSA, or another vendor suggested and USPS approved method for the creation and verification of digital signatures. If DSA or RSA are used, the PSD must adhere to the requirements specified in Section 3.1.1.1 for DSA or Section 3.1.1.2 for RSA and the appropriate government/commercial standards. Requirements for other approved digital signature methods, if any, will be documented in a future version of this specification.

3.1.1.1 Digital Signature Algorithm Requirements

If DSA is chosen, the PSD shall use the DSA, as specified in FIPS PUB 186, to implement digital signature generation and verification functions, using the standard DSA parameters that are defined in FIPS PUB 186. These functions process input messages in the formats specified in Section 3.2. Figure 3.1-1 illustrates the generic signature generation and verification processes. Applications of these processes to satisfy IBIP requirements are defined in Section 3.2.

The following sections, Section 3.1.1.1.1 and Section 3.1.1.1.2, detail requirements and parameters for the use of DSA. A PSD must adhere to the requirements addressed in these sections only if it implements DSA for IBIP.

3.1.1.1.1 PSD Digital Signature Algorithm Parameters

Using the default, standard parameters specified in FIPS PUB 186, the PSD shall obtain or generate, as appropriate, the DSA parameters listed in Table 3.1-1 for signature generation, and Table 3.1-2 for signature verification.

Figure 3.1-1. Digital Signature Generation and Verification

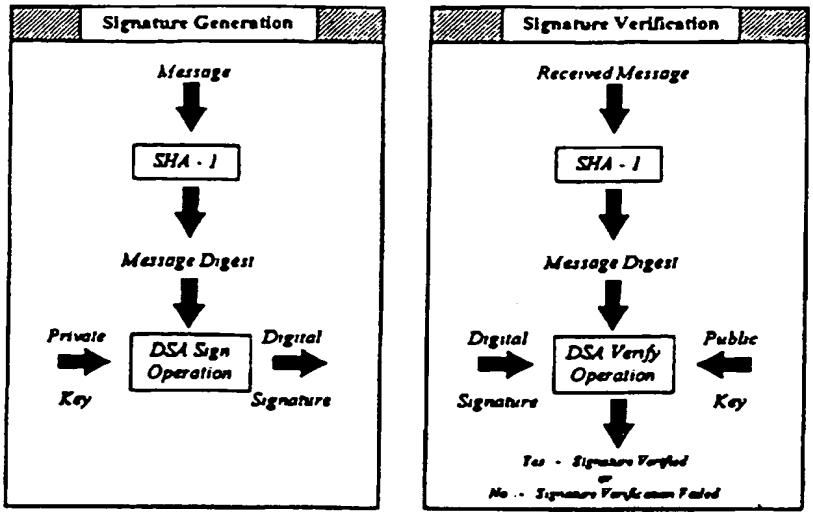


Table 3.1-1. DSA Parameters for Signature Generation

Parameter	Source	PSD Storage	Comments
p	Loaded into the PSD during device authorization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs
q	Loaded into the PSD during device authorization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs
g	Loaded into the PSD during device authorization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs
x	Generated by the PSD or loaded from external source	Stored in nonvolatile memory until replaced or erased	PSD private key
y	Calculated by the PSD if the x parameter is internally generated and output to host system	Not stored in the PSD	PSD public key
M	Message created by the PSD based on host system inputs and internal register contents	Stored in the PSD only for the duration of DSA signature generation	Output to host system by the PSD
k	Generated by the PSD	Used for a single signature erased after use	A new random value must be generated for each digital signature
r	Calculated by the PSD during the DSA sign operation	Result of DSA signature generation; erased after us	Output to host system by the PSD
s	Calculated by the PSD during the DSA sign operation	Result of DSA signature generation; erased after us	Output to host system by the PSD

3.1.1.1.2 PSD Secure Hash Algorithm

In accordance with FIPS PUB 186, the Secure Hash Algorithm (SHA-1), as specified in the Secure Hash Standard, FIPS PUB 180-1, shall be used to create a 160-bit message digest that is used in the creation of the digital signature.

Table 3.1-2. DSA Parameters For Signature Verification

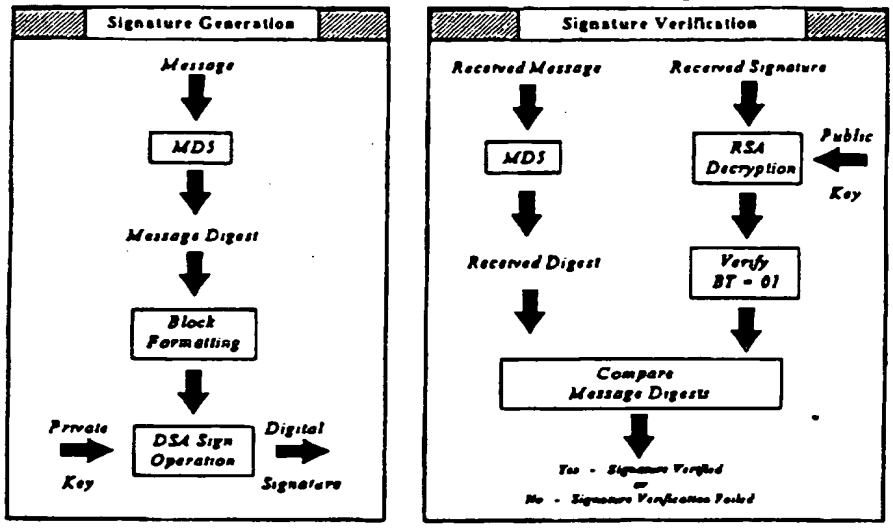
Parameter	Source	PSD Storage	Comments
p	Loaded into the PSD during device authorization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs (Same as p parameter for signatur generation)
q	Loaded into the PSD during device authorization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs (Same as q parameter for signature generation)
g	Loaded into the PSD during device authorization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs (Same as g parameter for signatur generation)
y	Loaded into the PSD from the host system	Stored in nonvolatile memory until replaced or erased	Public key of message originator
M'	Message as received from message originator	Stored in PSD only for duration of DSA signature verification	Input from the host system to the PSD
r'	r value received from message originator	Stored in PSD only for duration of DSA signature verification	Input from the host system to the PSD
s'	s value received from message originator	Stored in PSD only for duration of DSA signature verification	Input from the host system to the PSD
w, u1, u2, v	Generated by the PSD during signature verification process	Stored in PSD only for duration of DSA signature verification	The signature is verified if v=r'; PSD actions upon verification (or failure of verification) are specifie in Section 3.2

3.1.1.2 RSA Requirements

If RSA is chosen, the PSD shall use RSA as specified in PKCS #1 section 10, to implement digital signature generation and verification functions, using the standard RSA parameters that are defined in PKCS #1: RSA Encryption Standard. These functions process input messages in the formats that are specified in Section 3.2. Figure 3.1-2 illustrates the generic signature generation and verification processes. Applications of these processes to satisfy IBIP requirements are defined in Section 3.2.

The following sections, Section 3.1.1.2.1 and Section 3.1.1.2.2, detail requirements and parameters for the use of RSA. A PSD must adhere to the requirements addressed in these sections only if it implements RSA for IBIP.

Figure 3.1-2. RSA Digital Signature Generation and Verification



3.1.1.2.1 PSD RSA Digital Signature Parameters

If RSA is used, the PSD shall generate the appropriate parameters, listed in Table 3.1-3 for RSA signature generation and Table 3.1-4 for RSA signature verification.

Table 3.1-3. RSA Parameters for Signature Generation

Parameter	Source	PSD Storage	Comments
p	Generated by the PSD during device authorization	N/A	Needed to calculate the PSD's modulus n
q	Generated by the PSD during device authorization	N/A	Needed to calculate the PSD's modulus n
n	Modulus for the PSD, calculated during authorization	Stored in nonvolatile memory until replaced or erased	n=pq, stored as part of the PSD's public key
e	Generated by the PSD during device authorization	Stored in nonvolatile memory until replaced or erased	PSD's private key
d	IBIP established parameter	Stored in nonvolatile memory until replaced or erased	RSA exponential value used in the signature verification process
S	Generated during the RSA signature generation process	Stored in PSD only for duration of RSA signature generation	Result of the RSA signature generation that is output to the hos system

Table 3.1-4. RSA Parameters for Signature Verification

Parameter	Source	PSD Storage	Comments
n	X.509 Certificate of the signer	Stored in nonvolatile memory until replaced or erased	Part of the signer's public key
d	IBIP established parameter	Stored in nonvolatile memory until replaced or erased	
M	Message generated by the sender	Stored in PSD only for duration of RSA signature verification	n=pq, stored as part of the PSD's public key
S	Generated by the message originator during message creation	Stored in PSD only for duration of DSA signature verification	
MD	Message digest from the signature of the message	Stored in PSD only for duration of DSA signature verification	Input from the host system to the PSD
MD'	Generated using the received message during the RSA signature generation process	Stored in PSD only for duration of RSA signature verification	RSA signature is verified if MD'=MD

3.1.1.2.2 RSA Message Digest

The MD5 Message Digest Algorithm, as specified in RFC 1321, shall be used to create a 128 bit message digest for use in the digital signature process.

3.1.2 PSD Register Management Functions

The PSD shall store and increment ascending and descending registers in nonvolatile memory to support the IBIP finance, indicium creation, and device audit functions as discussed in Section 3.2. The management of these registers is specified in this section.

3.1.2.1 PSD Register Formats

Each register will represent a monetary value. The monetary values shall be measured in 1/10 of one cent increments. The ascending register shall consist of twelve numeric digits. The descending register shall consist of nine numeric digits. Therefore, the register values shall be interpreted as follows:

- Ascending Register: $XXX,XXX,XXX.XXX
- Descending Register: $XXX,XXX.XXX

The ascending register will support any value up to $1 billion and the descending register any value up to $1 million. (The maximum dollar value that may be loaded into the descending register will be established by USPS policy.)

3.1.2.2 PSD Register Operations

When the PSD receives a postage value download message resulting from the IBIP finance function and that message has been validated as discussed in Section 3.2, the PSD shall check for the replay of prior postage value download messages by comparing the old control total field in the postage value download message with the sum of the ascending and descending registers in the PSD. When the control total in the download message equals the sum of the values of the ascending and descending registers, the descending register value shall be increased by the amount of the postage value contained in the download message. If the control total in the download message does not equal the sum of the values in the ascending and descending registers, the PSD shall abort the download process and send an appropriate message to the host system.

When the host system requests the creation of an indicium, the PSD shall perform several operations using the ascending and descending registers. First, the PSD shall compare the requested postage amount input from the host system with the allowable limits currently in effect. If the requested postage amount is greater than or equal to the minimum limit and less than or equal to the maximum limit, the PSD will proceed with its register management functions. The requested postage amount shall then be compared to the value contained in the descending register. When the descending register contains sufficient value, the register values shall change in accordance with Table 3.1-5. If an insufficient value remains in the descending register, the PSD shall return an appropriate message to the host system and abort the indicium creation function.

Table 3.1-5. Ascending and Descending Register Operations

IBIP Function	Ascending Register Operation	Descending Register Operation
Indicium Creation	The value contained in the ascending register shall increase by the postage amount specified by the host system	The value contained in the descending register shall decrease by the postage amount specified by the host system
Finance (Upon receipt of postage value download message by the PSD)	The value contained in the ascending register shall be unchanged by the finance function	The value contained in the descending register shall increase by the amount of postage value contained in a valid postage value download message

3.1.2.3 Register Integrity

After completion of the initialization of the PSD, the PSD shall have no mechanism available to either the vendor or the customer to alter the value contained in the ascending register except as specified in Section 3.1.2.2.

The PSD shall have no mechanism to alter the value contained in the descending register except as specified in Section 3.1.2.2.

Upon request of the host system, the current value of the descending register shall be output to the host system for display to the user. This function will allow the user to determine the remaining postage value contained in the PSD. The host system shall have no mechanism to alter the ascending and descending register values in the PSD.

3.1.3 PSD Initialization

The initialization of a PSD includes loading the vendor's public key and the PSD device ID. In addition, the PSD shall explicitly initialize all internal registers, counters, etc., to their intended initial values.

The private key, which corresponds to the vendor's public key, will be used by the vendor to digitally sign selected information that is loaded into the PSD. At a minimum, the information to be signed shall include the PSD device ID (see section 3.1.3.2) and all IBIP device authorization information (see section 3.2.1). This key also may be used to sign other vendor-defined information that must be loaded into the PSD. The vendor shall define the specific format of the data to be signed for input into the PSD.

If DSA or RSA are used, the PSD shall use the signature verification function specified in either the DSS and Section 3.1.1.1 or the RSA PKCS and section 3.1.1.2 to verify the authenticity of the information loaded into the PSD. If the verification process fails, the information shall be discarded without further processing and an appropriate error indication shall be returned to the host system.

3.1.3.1 Load Vendor Public Key

The PSD shall be loaded by the vendor with the vendor's X.509 certificate, which contains the vendor's public key. This key shall be placed in nonvolatile storage in the PSD. The PSD shall have a mechanism to preclude the reloading or erasure of this key unless a new vendor X.509 certificate is received signed by the USPS.

3.1.3.2 Load PSD Device ID

Each PSD shall be loaded with a unique device ID, which will be based on a 3-digit vendor ID, a 3-digit model number, and an 8-digit PSD serial number. The USPS will assign the vendor ID. The USPS will assign the model numbers based on recommendations made by the vendor. The vendor shall assign a unique PSD serial number to each PSD during the manufacturing process. Any revisions to the PSD, including software upgrades to existing PSDs, shall result in a new 3-digit model number, making it necessary to load the new device ID into the PSD.

3.1.3.3 PSD Register Initialization

When the PSD is initialized by the PSD manufacturer, the values of both the ascending and descending registers shall be set to $000,000,000.000 and $000,000.000, respectively.

3.2 PSD Requirements to Implement IBIP Functional Requirements

This section presents the requirements for the proper implementation of IBIP functions. Where appropriate, reference is made to the core PSD functional requirements presented in Section 3.1.

3.2.1 IBIP Device Authorization Requirements

During the IBIP customer authorization process, the vendor will tailor the PSD for a particular customer and fully enable it to perform IBIP functions. This tailoring process is referred to as "device authorization" in this specification.

Prior to performing the device authorization functions, the PSD must have been initialized in accordance with Section 3.1.4 of this specification. PSD device authorization shall include the steps identified in the following subsections.

A vendor may reprogram a PSD with new device authorization information if the relevant customer authorization information changes (e.g., new address or device is re-issued with a new lease). The vendor must reprogram a PSD with the appropriate device authorization information if the PSD is issued to a different customer by the vendor.

3.2.1.1 Digital Signature Algorithm (DSA) Parameter Loading

If the PSD supports DSS, the PSD shall be loaded with the IBIP common DSA parameters (i.e., p, q, and g). The DSA parameters shall be stored in the appropriate nonvolatile memory location in the PSD. (These parameters must be obtained by the vendor from the IBIP certification authority in accordance with the IBIP system specification.)

3.2.1.2 Private/Public Key Processing

The PSD shall internally generate its own private key upon command from the vendor. The PSD shall calculate its public key based on its private key in compliance with FIPS PUB 186.

If the PSD implements the RSA algorithm, the PSD shall first generate its public key and then calculate its corresponding private key. The PSD shall output the public key to the vendor's host system. (The vendor will be responsible for passing the public key to the IBIP certification authority.)

The PSD private key shall be stored in the appropriate nonvolatile memory location in the PSD. The X.509 Certificate, containing the PSD's public key, shall be loaded into and stored in the PSD and/or the host system. This implementation is vendor specific.

3.2.1.3 Customer Identification Loading

The PSD shall be loaded with the customer license ID number and the 12-digit value to be placed in the originating address field in each indicium.

3.2.1.4 USPS X.509 Certificate Loading

The PSD shall be loaded with the X.509 certificate of the USPS that is obtained from the IBIP certification authority. The PSD shall use the signature verification process that is specified in section 3.1.1 to validate that the USPS X.509 certificate was received without modification. The format of the USPS X.509 certificate is provided in the IBIP system specification. Subsequent to successful verification of this certificate, the public key that is contained in the certificate will be used to verify signatures on postage value download messages and other messages that are received from the USPS.

3.2.1.5 Maximum/Minimum Postage Amount Loading

The PSD shall be loaded with the maximum and minimum postage values that the PSD will be allowed to process. These USPS-determined values stipulate the allowable range of the postage amount that a PSD is authorized to apply to an indicium. Additionally, the PSD shall have a mechanism to permit the printing of zero postage as specified in the DMM.

The PSD shall have a mechanism to update the maximum and minimum allowable postage range when the USPS changes postage rates.

3.2.1.6 Watchdog Timer Reset Value

The initial value of the watchdog timer shall be set by the vendor at authorization. The PSD shall be loaded with a value, which is measured in days, that will be used as the reset value of the watchdog timer.

3.2.2 IBIP Finance Functions

The fundamental role of the PSD in the implementation of the IBIP finance functions is to request, accept, and process postage value download messages in accordance with the IBIP system specification. The process is illustrated in Figure 3.2-1. To support IBIP finance functions, messages originating from the PSD must be transferred to the IBIP infrastructure, and messages from the IBIP infrastructure must be transferred to the PSD. The specific transfer mechanisms for these messages are beyond the scope of this specification and may vary.

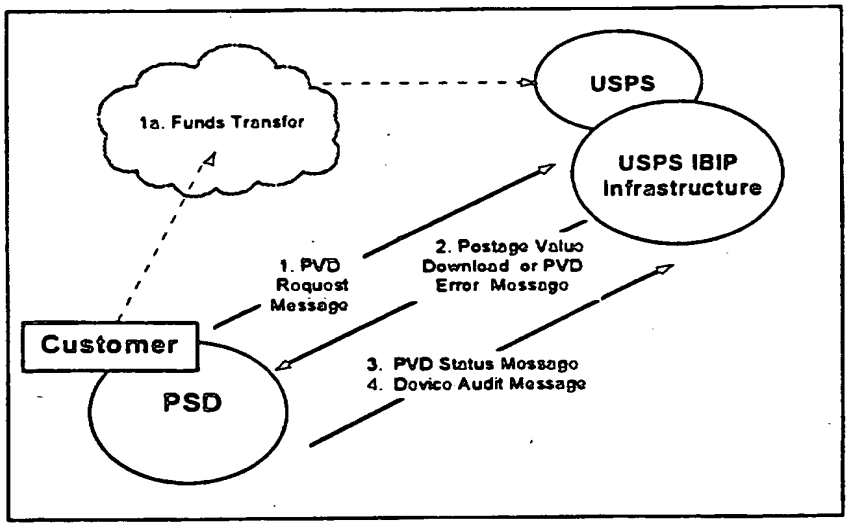
When a customer needs to add postage value to their PSD, the customer must have sufficient funds on deposit with the USPS. The customer will not be able to add postage value to the PSD until sufficient funds are on deposit. If necessary, the customer must execute a funds transfer to the USPS.

The PSD will initiate the postage value download process with an appropriate request message to the USPS IBIP infrastructure. As part of the request message, the PSD will assign a unique 6-digit transaction ID number to the request. The transaction ID number will be used in the resulting postage value download, error, and status messages to associate those messages with the original request message.

Upon receipt of the request message, the IBIP infrastructure will check for sufficient funds and compare the PSD-originated information with the corresponding information contained in the IBIP databases. Successful checks result in a Postage Value Download (PVD) message to the PSD, or if a check fails, a PVD error message. Once the PSD receives and processes its added postage value message, it will reply with a postage value download status message to indicate successful or failed processing to the IBIP infrastructure. Requirements for messages processed by the PSD are further specified in the subsections that follow.

The PSD shall complete its role in the process by sending a device audit message, described in Section 3.2.4, to the IBIP infrastructure and resetting its watchdog timer. The PSD vendor shall define an approach to resolve failures during the postage download process.

Figure 3.2-1. IBIP Finance Function Process



3.2.2.1 Postage Value Download Request Message

The PSD shall initiate the postage download process by creating a request message, as described in this section, and passing that message to the host system for transmission to the IBIP infrastructure.

3.2.2.1.1 Postage Value Download Request Message Format

The request message for download of postage value shall contain the fields, sizes, and formats that are indicated in Table 3.2-1. However, the size of the digital signature and the PSD X.509 certificate fields may vary if the vendor implements another USPS-approved digital signature approach. Each request message shall be assigned a unique transaction ID number by the PSD. The transaction ID number and the amount of requested additional postage value shall be stored in the PSD for comparison with the corresponding fields in the received postage value download message.

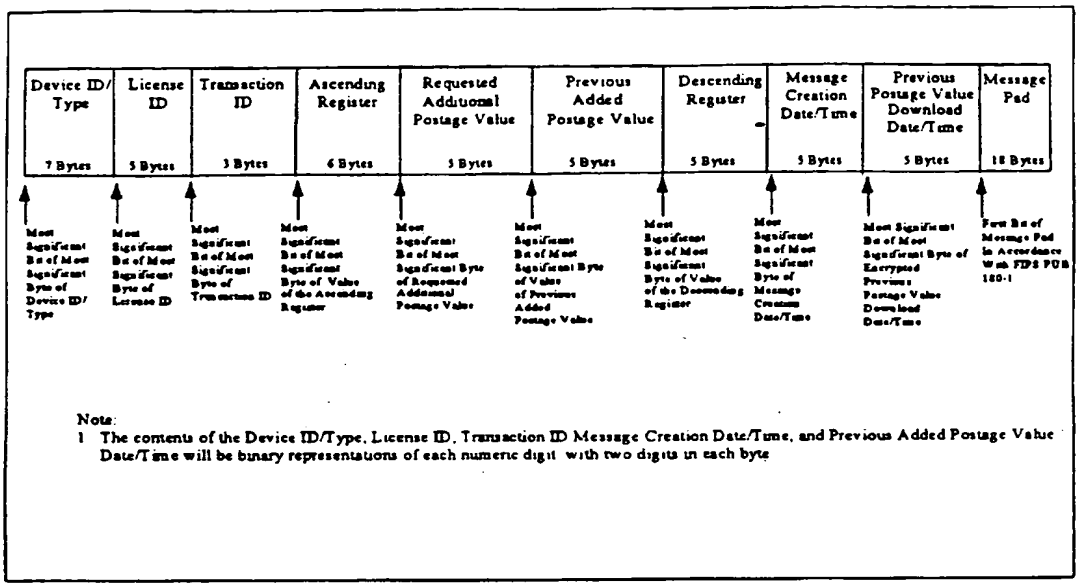
Table 3.2-1. Postage Value Download Request Message Format

Field Name	Size		Comments
Device ID/Type	7 bytes		The requesting PSD device ID/type number
License ID	5 bytes		The license ID associated with the requesting PSD
Transaction ID	3 bytes		A counter maintained internally by the PSD that is incremented with each postage value download request
Requested Additional Postage Value	5 bytes		The requested additional postage value consists of nine numeric digits in a 5-byte field
Ascending Register	6 bytes		Value of the ascending register
Descending Register	5 bytes		Value of the descending register
Message Creation Date/Time	5 bytes		Date and time that the message was created, in format YYMMDDHHMM
Previous Added Postage Value	5 bytes		Added postage value amount from the most recent postage value download transaction
Previous Postage Value Download Date/Time	5 bytes		Date/time that the most recent postage value download transaction was processed
Digital Signature	DSA 40 bytes	RSA 128 bytes	The digital signature that will be used to verify that the message was not altered enroute to the USPS. For DSA, the first 20 bytes of this field will contain the r value and the last 20 bytes will contain the s value.
PSD X.509 Certificate	DSA 235 bytes	RSA 323 bytes	The X.509 Certificate containing the public key necessary to verify the digital signature.

3.2.2.1.2 Postage Value Download Request Message Signature Generation

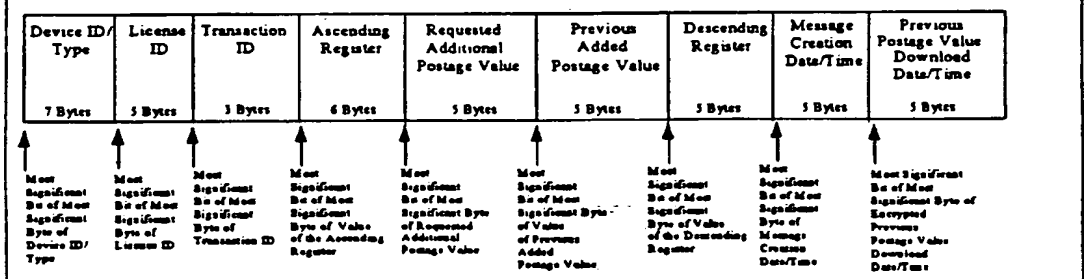
The digital signature for the postage value download request message shall be created by the PSD, as specified in Section 3.1.1 of this specification. If DSA is implemented, the input message for the digital signature process is shown in Figure 3.2-2. If RSA is implemented, the input message for the digital signature process is shown in Figure 3.2-3.

Figure 3.2-2. Input for the Postage Value Download Request Signature Generation Using DSA



Note:
1 The contents of the Device ID/Type, License ID, Transaction ID Message Creation Date/Time, and Previous Added Postage Value Date/Time will be binary representations of each numeric digit with two digits in each byte

Figure 3.2-3. Input for the Postage Value Download Request Signature Generation Using RSA



Note:
1. The contents of the Device ID/Type, License ID, Transaction ID Message Creation Date/Time, and Previous Added Postage Value Date/Time will be binary representations of each numeric digit with two digits in each byte.

3.2.2.2 Postage Value Download Message

After the USPS IBIP infrastructure successfully checks for receipt of adequate funding from the PSD licensee and validates the audit data that is provided in the request message, it will prepare and return the additional postage value that was requested by the PSD in a postage value download message as described in this section.

3.2.2.2.1 Postage Value Download Message Format

The postage value download message will contain the fields, sizes, and formats indicated in Table 3.2-2. However, the size of the digital signature field may vary if the vendor implements another USPS-approved digital signature approach.

Table 3.2-2. Postage Value Download Message Format

Field Name	Size		Comments
Device ID/Type	7 bytes		The PSD shall only accept postage value messages containing the device ID/type number of that PSD
Transaction ID	3 bytes		The transaction ID from the postage value download request message
Old Control Total	6 bytes		The old control total, consisting of 12 numeric digits in a 6-byte field, is used to verify that the postage value download message has not previously been processed by the PSD
Added Postage Value	5 bytes		The added postage value consists of 9 numeric digits in a 5-byte field
Digital Signature	DSA 40 bytes	RSA 128 bytes	The digital signature will be used to verify that the message was not altered enroute to the PSD. For DSA, the first 20 bytes of this field will contain the r' value and the last 20 bytes will contain the s' value.

3.2.2.2.2 Postage Value Download Message Signature Validation

Upon receipt of a postage value download message from the host system, the PSD shall format the data for signature verification. If the PSD uses DSA or RSA, the data shall be formatted as shown in either Figure 3.2-4 or Figure 3.2-5 for input into the signature verification process. If the PSD implements DSA, the PSD shall extract the r' and s' values for the signature verification process from the digital signature field in the received postage value download message.

The PSDs implementing either DSA or RSA shall use the signature verification process defined in Section 3.1.1 to verify that the message was received without modification. If the verification process fails, the message shall be discarded without further processing, and an appropriate error indication shall be returned to the host system.

Figure 3.2-4. Input Format for Postage Value Download Signature Verification (Received message, M', as defined in the DSS)

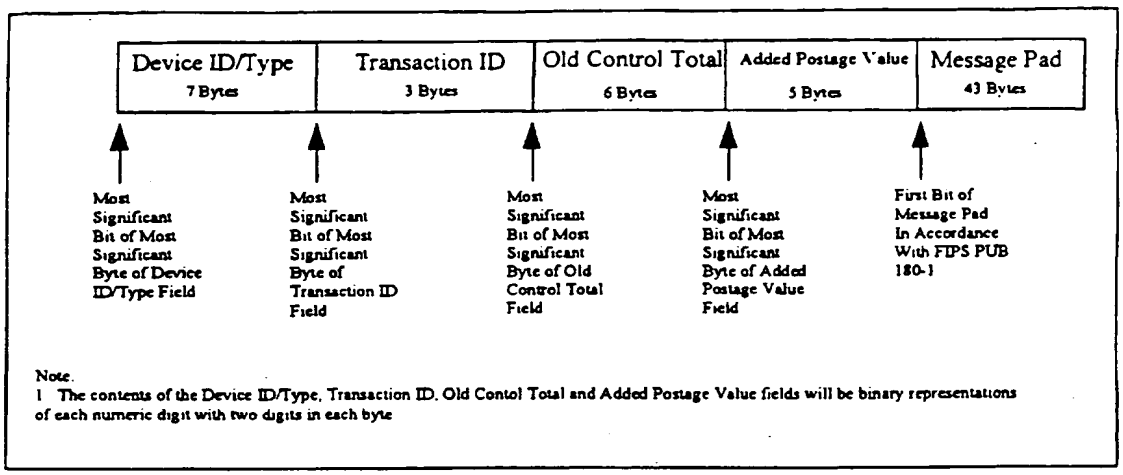
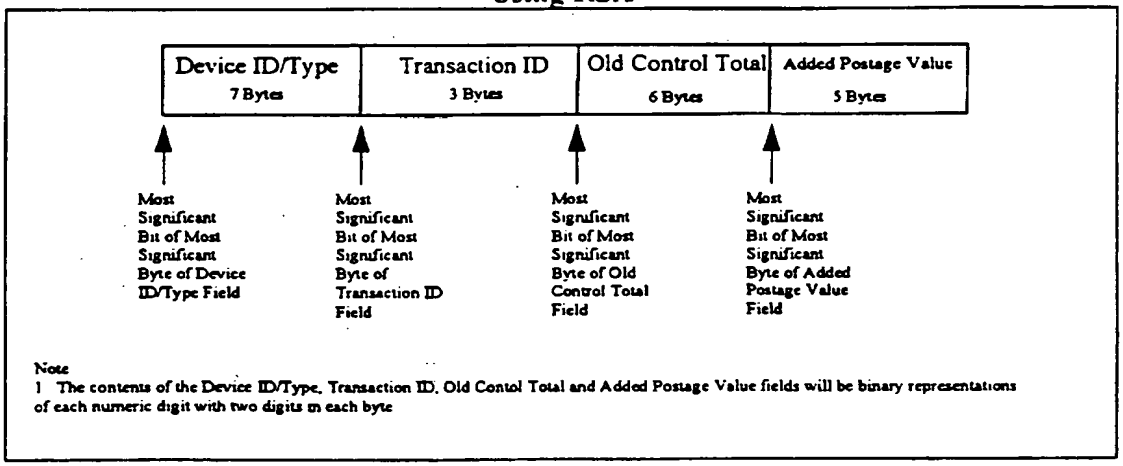


Figure 3.2-5. Input Format for Postage Value Download Signature Verification Using RSA



3.2.2.2.3 Postage Value Download Message Processing

After the signature verification process has been completed, the PSD shall compare the received transaction ID number with the pending request message transaction ID number. If these match, the PSD shall process the message in accordance with Section 3.1.2.2 of this specification. If the transaction ID numbers do not match or if there was no pending

request message, the PSD shall abort the processing of the download message and create an appropriate status message in accordance with Section 3.2.2.3 of this specification.

3.2.2.3 Postage Value Download Status Message

To acknowledge the success or failure of the processing of the postage value download message, the PSD shall create a status message for transmission to the USPS.

3.2.2.3.1 Postage Value Download Status Message Format

The status message shall contain the fields, sizes, and formats that are indicated in Table 3.2-3. However, the size of the digital signature and the PSD X.509 certificate fields may vary if the vendor implements another USPS-approved digital signature approach.

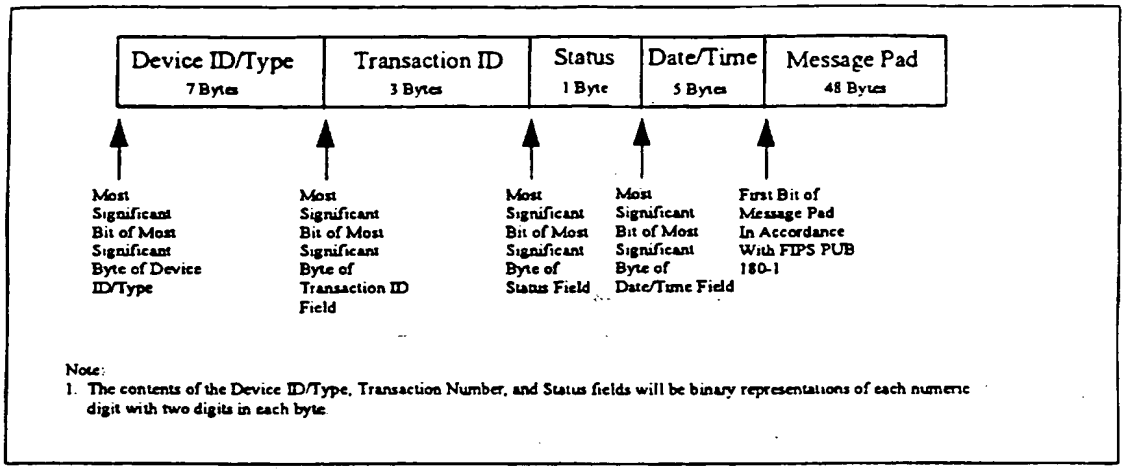
Table 3.2-3. Postage Value Download Status Message Format

Field Name	Size		Comments
Device ID/Type	7 bytes		The requesting PSD's Device ID/Type number
Transaction ID	3 bytes		The same Transaction ID included in the original PVD request message and returned in the PVD message
Status	1 byte		Applicable status numbers are TBD
Date/Time	5 bytes		The date and time the PSD completed the postage value download or encountered any errors
Digital Signature	DSA 40 bytes	RSA 128 bytes	The digital signature will be used to verify that the message was not altered enroute to the USPS. For DSA, the first 20 bytes of this field will contain the r' value. The last 20 bytes will contain the s' value.
PSD X.509 Certificate	DSA 235 bytes	RSA 323 bytes	The X.509 Certificate containing the public key necessary to verify the digital signature.

3.2.2.3.2 Postage Value Download Status Message Signature Generation

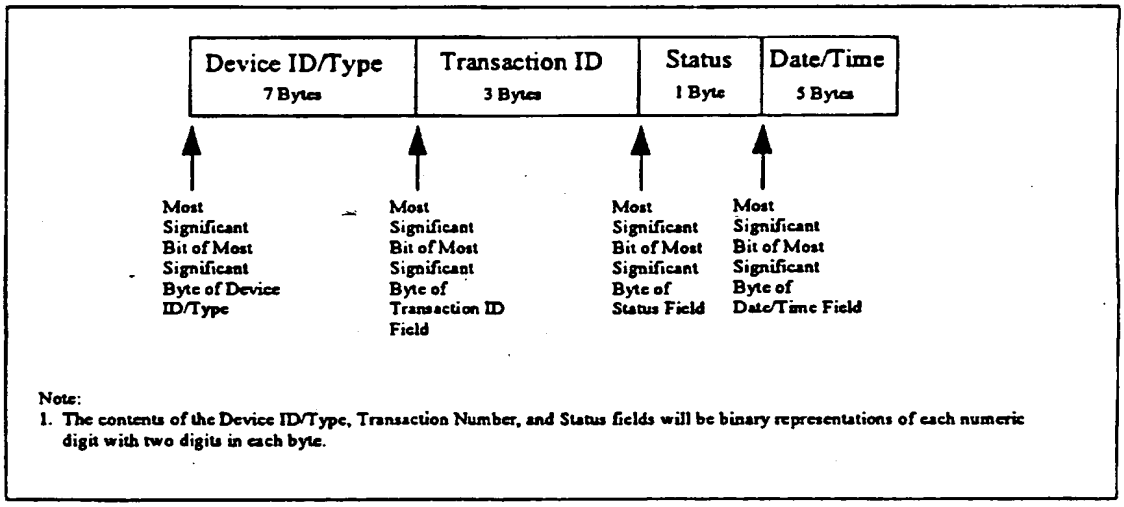
The digital signature for the postage value download status message shall be created by the PSD as specified in Section 3.1.1 of this specification. If the PSD implements DSA, the input message for the digital signature process is shown in Figure 3.2-6. If the PSD implements RSA, the digital signature input message is shown in Figure 3.2-7 .

Figure 3.2-6. DSA Input for PVD Status Message Signature Generation



Note:
1. The contents of the Device ID/Type, Transaction Number, and Status fields will be binary representations of each numeric digit with two digits in each byte.

Figure 3.2-7. RSA Input for PVD Status Message Signature Generation



Note:
1. The contents of the Device ID/Type, Transaction Number, and Status fields will be binary representations of each numeric digit with two digits in each byte.

3.2.2.4 Postage Value Download Device Audit Message

Subsequent to the processing of the postage value download message and the creation of the status message, the PSD shall generate a device audit message as specified in Section 3.2.4.

3.2.2.5 Postage Value Download Error Message

The IBIP infrastructure will return an error message to the PSD in response to a postage value download request message that fails validation, as discussed in this section.

3.2.2.5.1 Postage Value Download Error Message Format

The postage value download error message shall contain the fields, sizes, and formats that are indicated in Table 3.2.4. However, the size of the digital signature field may vary if the vendor implements another USPS-approved digital signature approach.

Table 3.2-4. Postage Value Download Error Message Format

Field Name	Size		Comments
Device ID/Type	7 bytes		The requesting PSD's device ID/type number
Transaction ID	3 bytes		The transaction ID from the postage value download request message
Error Code	1 byte		Applicable error codes are TBD
Digital Signature	DSA 40 bytes	RSA 128 bytes	The digital signature will be used to verify that the message was not altered enroute to the PSD. For DSA, the first 20 bytes of this field will contain the r' value and the last 20 bytes will contain the s' value.

3.2.2.5.2 Postage Value Download Error Message Signature Verification

Upon receipt of a postage value download error message from the host system, the PSD shall format the data for signature verification. If the PSD uses DSA or RSA, the data shall be formatted as shown in either Figure 3.2-8 or Figure 3.2-9 for input into the signature verification process. If the PSD implements DSA, the PSD shall extract the r' and s' values for the signature verification process from the digital signature field in the received postage value download message.

The PSDs implementing either DSA or RSA shall use the signature verification process defined in Section 3.1.1 to verify that the message was received without modification. If the verification process fails, the message shall be discarded without further processing, and an appropriate error indication shall be returned to the host system.

Figure 3.2-8. Input for Postage Value Download Error Message Signature Verification using DSA

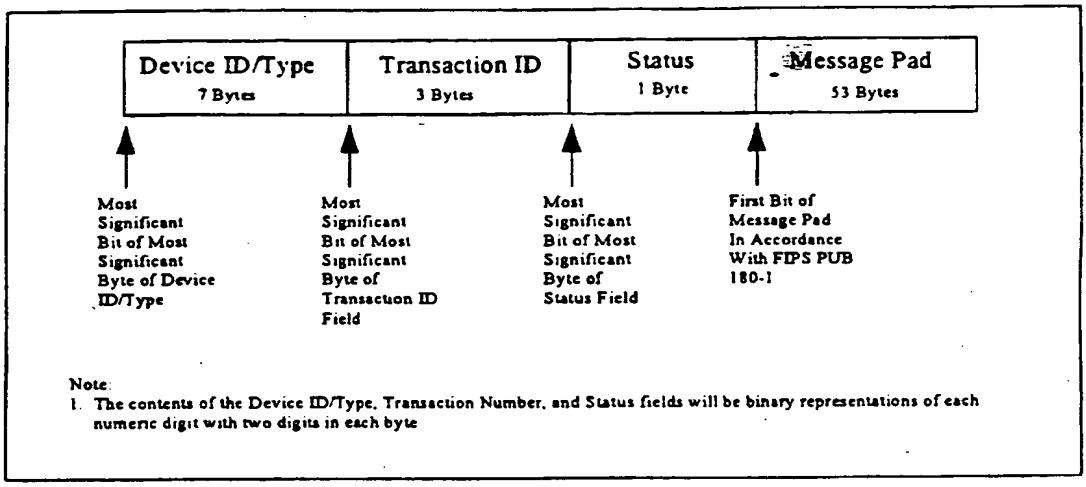
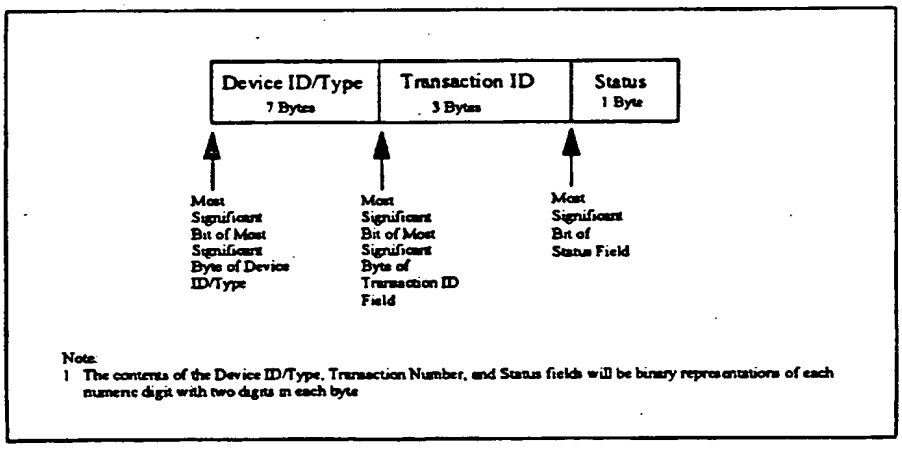


Figure 3.2-9. Input for Postage Value Download Error Message Signature Verification using RSA



3.2.3 Indicium Creation Function

The role of the PSD in the IBIP indicium creation function is to perform security-critical processes as described in this section. It is the responsibility of the host system to appropriately use the information provided by the PSD to create the indicium. If any of the processes described in this section fails the PSD shall issue an appropriate error message to the host system.

3.2.3.1 Indicium Creation Host Request

The PSD shall accept a request from the host system to perform the security functions that are necessary for the host to create an indicium. The format of this request is at the discretion of the PSD vendor but shall consist minimally of the requested postage amount and the special purpose field, as defined in the IBIP Indicium Specification.

3.2.3.2 Indicium Creation Register Operations

The PSD shall perform the maximum and minimum limit checks and register operations in accordance with Section 3.1.2.2 of this specification before signing the register values.

3.2.3.3 Indicium Creation Signature Generation

The PSD shall generate a digital signature for the indicium as defined in the IBIP Indicium Specification and Section 3.1.1 of this specification. Additional digital signature methods may be used only with USPS approval. The criteria for the approval are defined in the IBIP Indicium Specification Section 4.4.

3.2.3.4 Indicium Creation Results Output

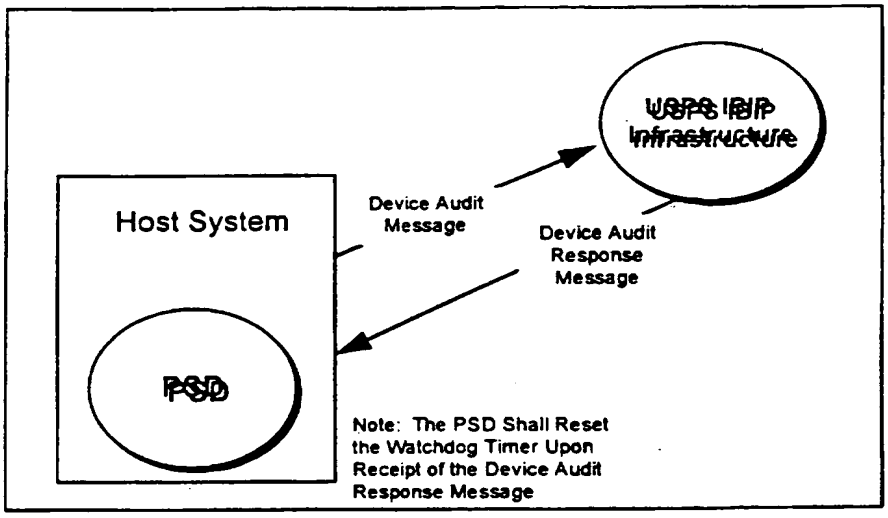
Upon successful completion of the processes defined in Sections 3.2.3.1 through 3.2.3.4, the PSD shall output the following fields to the host system: ascending register, descending register, and the digital signature. It will be the responsibility of the host system to generate the bar code portion of the indicium.

3.2.4 Device Audit Function

The primary role of the PSD in the device audit function is to create device audit messages and pass those messages to the host system for transmission to the USPS. The PSD shall initiate the device audit function upon host request and to request the reset of a "timed out" watchdog timer. The PSD also shall automatically create and send an audit message with the postage value download status message after processing a postage value download message.

The overall device audit process is illustrated in Figure 3.2-10. Upon receipt of a device audit message other than one received as the final step in the postage value download process, the USPS IBIP infrastructure will create a device audit response message and return that message to the PSD. After validating the response message, the PSD shall reset the watchdog timer to its initial value.

Figure 3.2-10. Device Audit Process



3.2.4.1 Device Audit Message

Device audit messages created by the PSD shall conform to the requirements contained in this section.

3.2.4.1.1 Device Audit Message Contents

The PSD shall create device audit messages that contain the fields, sizes, and formats indicated in Table 3.2-5, however the size of the digital signature and the PSD X.509 certificate fields may vary if the vendor implements another USPS-approved digital signature approach.

For device audit messages created as the final step in the postage value download process, the transaction ID from the postage value download message shall be used. For all other device audit messages, a unique transaction ID shall be generated. The PSD shall assign transaction ID numbers for device audit messages in a manner similar to that for postage value download request messages.

Table 3.2-5. Device Audit Message Format

Field Name	Size		Comments
Device ID/Type	7 bytes		The originating PSD Device ID/Type number
Transaction ID	3 bytes		An identification number for this device audit message
Ascending Register	6 bytes		Value of the ascending register
Descending Register	5 bytes		Value of the descending register
Audit Message Creation Date/Time	5 bytes		Date and time the audit message was created in format YYMMDDHHMM
Previous Added Postage Value	5 bytes		Added Postage Value amount from the most recent postage value download message
Previous Postage Value Download Date/Time	5 bytes		Date/time that the most recent postage value download message was processed
Digital Signature	DSA 40 bytes	RSA 128 bytes	The digital signature will be used to verify that the message was not altered enroute to the PSD. The first 20 bytes of this field will contain the r' value and the last 20 bytes will contain the s' value
PSD X.509 Certificate	DSA 235 bytes	RSA 323 bytes	The X.509 Certificate containing the public key necessary to verify the digital signature

3.2.4.1.2 Device Audit Message Signature Generation

The PSD shall generate a digital signature for the device audit message as defined in Section 3.1.1 of this specification. If DSA is implemented, the input message for the signature generation function is shown in Figure 3.2-11. If RSA is implemented, the input message for the signature generation is shown in Figure 3.2-12.

Figure 3.2-11. DSA Input Format for Device Audit Signature Generation

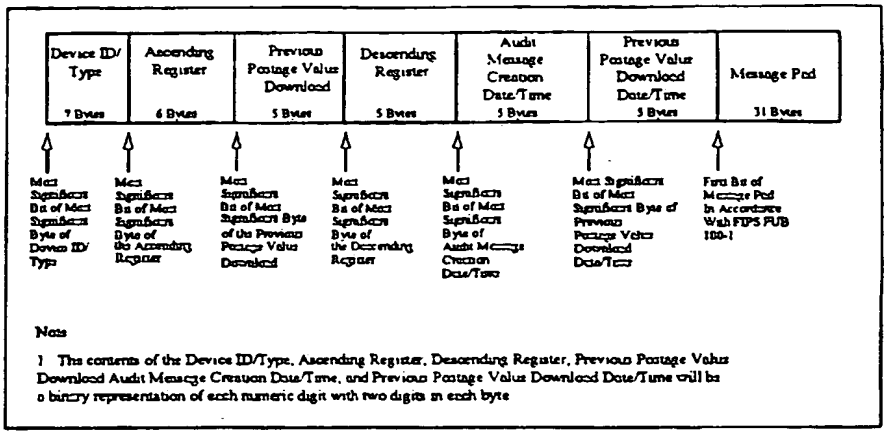
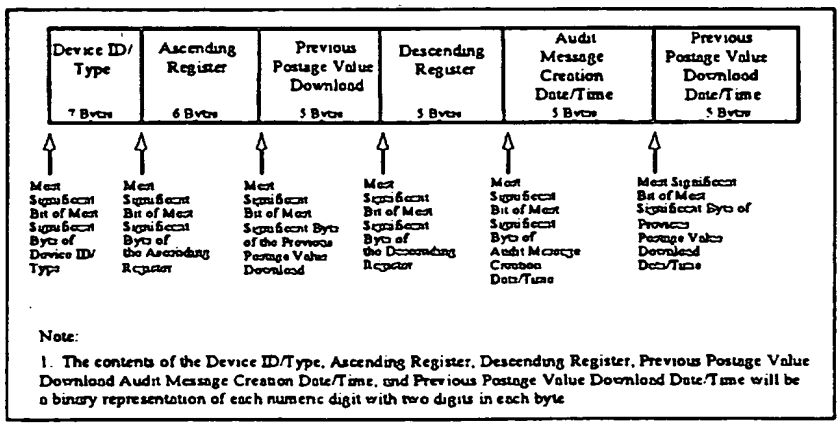


Figure 3.2-12. RSA Input Format for Device Audit Signature Generation



3.2.4.2 Device Audit Response Message

The IBIP infrastructure will return a device audit response message to the PSD in response to the receipt of a device audit message unless the device audit message was received as the final step in the postage value download process. The processing of the device audit response message by the PSD is specified in this section.

3.2.4.2.1 Device Audit Response Message Format

The device audit response message shall contain the fields and sizes indicated in Table 3.2-6, however the size of the digital signature field may vary depending on the digital signature method implemented by the PSD.

Table 3.2-6. Device Audit Response Message Format

Field Name	Size		Comments
Device ID/Type	7 bytes		The PSD's device ID/type number
Transaction ID	3 bytes		The transaction ID from the device audit message
Status Code	1 byte		Applicable status codes are TBD
Digital Signature	DSA 40 bytes	RSA 128 bytes	The digital signature will be used to verify that the message was not altered enroute to the PSD. For DSA, the first 20 bytes of this field will contain the r' value and the last 20 bytes will contain the s' value

3.2.4.2.2 Device Audit Response Message Signature Verification

Upon receipt of a device audit response message from the host system, the PSD shall format the data for signature verification. If the PSD uses DSA or RSA, the data shall be formatted as shown in either Figure 3.2-13 or Figure 3.2-14 for input into the signature verification process. If the PSD implements DSA, the PSD shall extract the r' and s' values for the signature verification process from the digital signature field in the received postage value download message.

The PSDs implementing either DSA or RSA shall use the signature verification process that is defined in Section 3.1.1 to verify that the message was received without modification. If the verification process succeeds, the PSD shall reset its watchdog timer to its initial value. If the verification process fails, the PSD shall discard the device audit response message without further processing and shall return an appropriate error indication to the host system.

Figure 3.2-13. Input for Device Audit Response Message Signature Validation

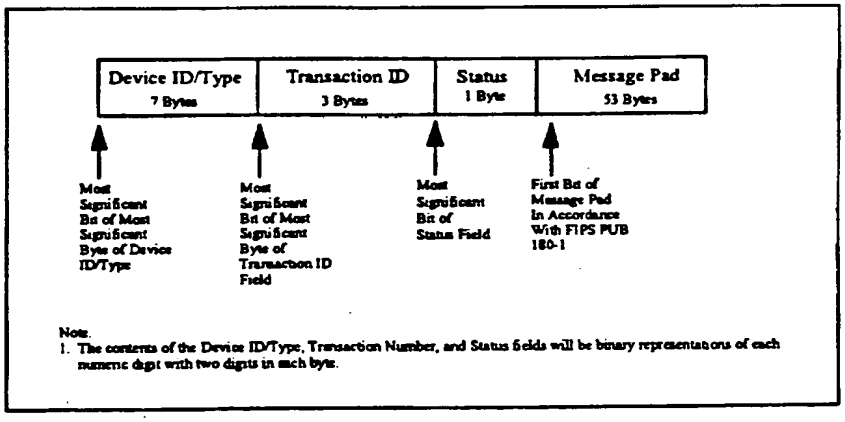
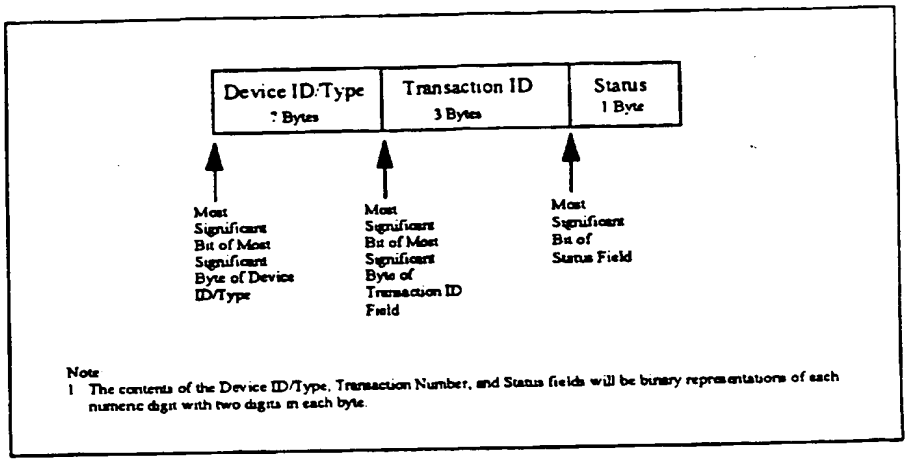


Figure 3.2-14. RSA Input for Device Audit Response Message Signature Validation



4. PSD PHYSICAL REQUIREMENTS

This section describes the physical requirements to which PSD shall conform. It is not the intent of this specification to require a particular physical form factor. The requirements presented in this section are those necessary to ensure the integrity of the PSD and the IBIP system.

4.1 PSD Security

The PSD shall be designed and implemented in accordance with FIPS PUB 140-1. The PSD shall conform to the requirements for security level 3 or as defined in Table 4.1-1.

Table 4.1-1. FIPS PUB 140-1 Requirements Applicable to PSD

FIPS 140-1 Design Category	Proposed PSD Specification / FIPS 140-1 Requirements	Comment
Crypto Module	Documentation Required: • PSD Module Description (by vendor) • Specification of PSD cryptographic module and its cryptographic boundary (by vendor) • PSD security policy (by vendor)	Vendor PSD description and specification must comply with this PSD Specification; vendor PSD security policy must comply with IBIP Security Policy
Module Interfaces	Paths explicitly defined (by vendor): power and control paths (from host system) input data (through host system) separate inputs for data and plaintext security parameters (keys and access control data), or single input if security parameters are protected output data and status (to host system) optional; maintenance access (vendor proprietary)	Message and data formats are to comply with the definitions in this PSD Specification
Roles	Authorized roles • User (customer through host system) • Crypto officer (vendor) • Maintenance (vendor-required if optional maintenance port is implemented) Access control - authentication by role for user, vendor, or individual (optional)	Minimum access control shall satisfy security level 2 (role-based) access; security level 3 and 4 (individual) access is optional; at least a PIN/password entry is needed for either case.
Services	• Initiate and run self-tests • Output module status to host system • Output module alarms to host system • Accept host system controls • PSD core and IBIP functions • No bypass capability	Self-tests - see below
Finite State Machine Model	Comply with FIPS PUB 140-1, section 4.4 design and documentation requirements	Required documentation from vendor/manufacturer
Physical Security	Table 4.6-1, PSD Physical Security requirements	
Environmental Failure Protection or Testing (EFP/EFT)	Employ environmental failure protection features or undergo environmental failure protection testing for accreditation	Implemented to counter a potential tampering mode (especially voltage and temperature)

FIPS 140-1 Design Category	Proposed PSD Specification / FIPS 140-1 Requirements	Comment
Software Security	Required documentation: software design, relationship of design to security policy, and annotated complete source code Implement in high level language unless low level language essential or high level language not available	Additional documentation required from vendor/ manufacturer
Operating System Security	Not applicable	Required only if operator has means of loading device software
Key Management	• Key generation - Only internal generation of PSD's public and private keys • Key distribution - Public key distribution TBD • Key archiving - PSD public key sent to USPS upon generation/loading	No key extraction except PSD public key
Crypto Algorithms	Implement either DSS, RSA, or other USPS approved signature generation and verification algorithm	Vendor may need to obtain necessary rights to use
Electromagnetic Interference and Compatibility (EMI/EMC)	Comply with EMI/EMC requirements specified by FCC Part 15, Subpart J, Class B (i.e., for home use, conforms to security levels 3 and 4)	Primarily for compatibility with other electronic devices
Self-Tests	Statistical random number generator test performed during initialization and again at authorization. Power up self-tests: • Crypto algorithm (known answer) • Error detection code or authentication • Critical functions Conditional tests: TBD by vendor (pair-wise consistency, software/firmware load, manual key entry, continuous random number generator)	Testing must ensure proper operation of PSD functions

4.2 PSD Contents

The PSD shall include an FIPS 140-1 compliant random number generator.

The PSD shall include a real-time clock.

The PSD shall include a backup battery capable of maintaining the real-time clock and tamper detection/response circuitry for a minimum of five years from installation. Other means of ensuring the retention of anti-tamper functions, PSD data, and continued operation of the real-time clock in the absence of primary input power, which is in lieu of a battery, will be evaluated, if proposed.

The PSD shall output an alarm signal indication in the event of a low battery power level condition.

4.3 PSD Internal Storage

PSD internal storage shall satisfy the data requirements of Sections 3.1 and 3.2 of this specification. Table 4.3-1 lists the minimum data required by IBIP in nonvolatile storage.

Table 4.3-1. PSD Internal Storage

Item	Size
Device ID/Type	7 bytes
License ID	5 bytes
PSD Private Key	160 bits for DSA or 1024 bits for RSA
IBIP Common Parameters	TBD
Originating Address	11 digits
Maximum/Minimum Postage Values	2.5 bytes each
Ascending Register	12 digits
Descending Register	9 digits
Transaction ID	3 bytes
PSD X.509 Certificate	TBD
Vendor X.509 Certificate	TBD
USPS X.509 Certificate	TBD

4.4 PSD Software

The PSD shall comply with the FIPS PUB 140-1 software security requirements appropriate for its security level.

The PSD shall comply with the operating system requirements applicable in accordance with FIPS PUB 140-1.

If the PSD vendor chooses a remote method of modifying software in the PSD, the change message will require a signature verification by the PSD before the software is updated.

4.5 Watchdog Timer

The initial value of the watchdog timer shall be set by the vendor at authorization. The watchdog timer shall be tied to the real-time clock in the PSD. When the timer expires, the PSD shall be unable to create additional indicia. A PSD that is disabled shall be reset only upon receipt of a valid device audit response message as discussed in section 3.2.4 of this specification. A PSD that is disabled will retain its memory and not zeroize, but it cannot be used to create indicia until the device audit response message is received.

4.6 PSD Tamper Resistance

The PSD shall have an explicitly defined perimeter that establishes the physical bounds of the cryptographic module and the cryptographic boundary, including the processor for the software and/or firmware that executes the code. The requirements for different format options are summarized in Table 4.6-1.

Table 4.6-1. PSD Physical Security Requirements (per FIPS PUB 140-1)

Single Chip Module (stand-alone or embedded)	Multi-Chip Module	Multi-Chip Stand-Alone Module
Inherently tamper resistant (e.g., smart card)	ICs with interconnections, not within a protected enclosure (e.g., expansion boards/adapters)	ICs interconnected within protected enclosure (e.g., IC printed circuit board or ceramic substrate)
• Hard opaque removal resistant coating including or covering passivation • Tamper response and zeroization active when keyed • Include environmental failure protection (shutdown or zeroization, especially for temperature and voltage), or undergo environmental failure testing	• Strong non-removable enclosure • Completely within tamper detection envelope • Tamper response and zeroization circuitry active when keyed • Any ventilation holes/slits to include anti probe design (e.g., 90 degree bends) completely within tamper detection envelope • Include environmental failure protection (shutdown or zeroization, especially for temperature and voltage), or undergo environmental failure testing	• Strong removal-resistant enclosure, with tamper detection for entire envelope • Tamper response and zeroization circuitry active when keyed • Any ventilation holes/slits to include anti probe design (e.g., 90 degree bends) • Include environmental failure protection (shutdown or zeroization, especially for temperature and voltage), or undergo environmental failure testing

The PSD shall use tamper detection countermeasures that respond to tampering by disabling the PSD from further use until completion of a physical inspection by USPS. The PSD ascending and descending register values shall be retained at the values that were present when the tampering was detected.

The PSD shall not provide any capability to bypass the security services of the cryptographic module.

4.7 PSD Access Control

The PSD shall employ security mechanisms to restrict unauthorized physical access to the contents of the module, thereby deterring unauthorized use and unauthorized modification (including substitution) of the PSD.

The PSD shall directly or through the host system authenticate any person who is authorized to perform the role of operator of the PSD (FIPS PUB 140-1, Security Level 2 minimum requirement e.g., password or PIN).

4.8 PSD Key Handling

PSD key entry and output, distribution, and storage shall be in accordance with the IBIP System Specification, Appendix (TBD), PSD Key Management.

PSD keys shall be stored in plaintext form in the cryptographic module and shall not be accessible from outside the device.

The PSD shall include a mechanism to ensure that stored keys shall remain associated with the correct device ID.

The PSD shall provide the capability to zeroize all plaintext cryptographic keys and other unprotected security parameters within the module.

The PSD shall not output its private keys.

4.9 PSD Input and Output Requirements

The data ports for unencrypted, critical PSD-security parameters shall be physically separated from other data ports.

If plaintext authentication data (e.g., password or PIN) is used, the entry port shall be physically separate from any other cryptographic module data entry port and allow for direct entry of the data.

The PSD shall provide an output for indication of the status of the device.

5. PSD TESTING REQUIREMENTS

This section describes the testing requirements for the PSD.

The PSD shall be tested for conformance with FIPS PUB 140-1 through the Cryptographic Module Validation Program by a cryptographic module testing laboratory that is a member of an accredited National Voluntary Laboratory Accreditation Program and shall receive a validation certificate. In addition, the PSD shall be evaluated by the USPS and receive IBIP accreditation.

The PSD shall either employ environmental failure protection features or undergo environmental testing, as required by FIPS PUB 140-1, to the extent appropriate for its security level.

Upon authorization for service to a customer, the PSD shall be tested for proper time stamping, signature generation, indicium data creation and output, signature validation, and maintenance of required data in its data storage registers.

The PSD shall initiate and run self-tests to ensure proper operation in accordance with FIPS PUB 140-1.

APPENDIX A: LIST OF ACRONYMS

ANSI	American National Standards Institute
DMM	Domestic Mail Manual
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
IBIP	Information Based Indicia Program
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptographic Standards
PSD	Postal Security Device
SHA	Secure Hash Algorithm
USPS	United States Postal Service